UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/553,415	04/20/2000	Satoshi Obana	074273/0163	4649

22428 7590 12/09/2004

FOLEY AND LARDNER
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/553,415	OBANA, SATOSHI	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Office action is in response to the amendment filed on June 14, 2004. The original application contained claims 1 – 63. Per the received amendment, claims 1 - 63 have been amended, and no claims have been cancelled. Presently pending claims are 1 – 63.

Response to Arguments

2. Applicant's arguments, filed on June 14, 2004, have been fully considered but they are not persuasive because of the following reasons:

Regarding currently amended claim 1, the applicant argues that the cited prior art (Aikawa et al., U.S. Patent 5,835,727) does not disclose "a control section that changes an encrypting operation at a next encrypting stage *a* ***plurality of times*** when it is determined that the encrypting operation at the next encrypting stage should be changed." The presently amended claim differs from the original amended claim 1 because it states that the changing of the encrypting operation at the next encrypting stage is performed a plurality of times. This argument is not found persuasive because Aikawa discloses an encrypting/decrypting conversion apparatus that is capable of changing algorithms (encrypting operations) based on cipher keys and algorithm

parameters (random numbers) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10). Specifically, Aikawa discloses an encrypting/decrypting conversion apparatus for "inputting at least one cipher key, at least one algorithm parameter, and plain text data and outputting cipher text data, the apparatus comprising***: a plurality stage of encrypting conversion means***" (column 2 lines 16 – 37). Furthermore, Aikawa discloses "the total number N of encrypting conversion repetitions is called a round number (column 6 lines 1 – 10). Therefore, Aikawa does teach "changing an encrypting operation at a next encrypting stage a plurality of times when it is determined that the encrypting operation at the next encrypting stage should be changed." Further amendments to the independent claim 1 include the addition of the limitation that the determining section determines whether said intermediate data at the next encrypting stage should be changed depending on at least a plurality of random numbers, and the limitation that the control section changes the intermediate data at the next encrypting stage a plurality of times depending on a plurality of random numbers. Both of these limitations are disclosed by the cited prior art (Aikawa) following the same reasoning given above. Aikawa delineates determining changing the encryption algorithm at a next step depending on a plurality of random numbers (algorithm keys) and changing the intermediate data at the next encrypting stage depending on a plurality of random numbers (column 5 line 38 – column 6 line 65). Therefore, Aikawa does teach the additional and amended limitations in the independent claim 1, and the corresponding amendments/additions reciting the "plurality of random numbers" in the remaining claims.

Accordingly, the rejection for the pending claims 1 – 63 is respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-5, 8-12, 15-19, 22-26, 29-33, 36-40, 43-47, 50-54, and 57-61 are rejected under 35 U.S.C. 102(e) as being anticipated by Aikawa et al. (U.S. Patent 6,606,385).

Regarding claim 1, Aikawa discloses:

An encrypting apparatus comprising:

an encrypting operation section carrying out an encrypting operation to a plaintext using intermediate data at each of a plurality of encrypting stages of said encrypting operation to produce a ciphertext, wherein said encrypting operation section outputs encrypting stage data indicating an encrypting state at each of said plurality of

processing stages (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

a determining section determining whether said encrypting operation at a next encrypting stage should be changed, based on said encrypting stage data at a current encrypting stage from said encrypting operation section (column 2 line 42 – column 3 line 51, column 5 lines 1-67); and

a control section changing said encrypting operation at said next encrypting stage a plurality of times when it is determined that said encrypting operation at said next encrypting stage should be changed (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50),

wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting operation section (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein said control section changes said intermediate data at said next encrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 8, Aikawa discloses:

A decrypting apparatus comprising:

a decrypting operation section carrying out a decrypting operation, to a ciphertext using intermediate data at each of a plurality of decrypting stages of said decrypting operation to produce a plaintext, wherein said decrypting operation section outputs decrypting stage data indicating a decrypting state at each of said plurality of decrypting stages (Figure 12, column 9 lines 24-58);

a determining section determining whether said decrypting operation at a next decrypting stage should be changed, based on said decrypting stage data at a current decrypting stage from said decrypting operation section (Figure 12, column 9 lines 24-58); and

a control section changing said decrypting operation at said next decrypting stage a plurality of times when it is determined that said decrypting operation at said next decrypting stage should be changed (Figure 12, column 9 lines 24-58),

wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said decrypting operation section (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next decrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein said control section changes said intermediate data at said next decrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 15, Aikawa discloses:

An encrypting and decrypting apparatus comprising:

an encrypting and decrypting operation section determining whether an inputted instruction is an encrypt instruction or a decrypt instruction, carrying out an encrypting operation to an inputted text in response to said encrypt instruction using first intermediate data at each of a plurality of encrypting stages of said encrypting operation to produce a ciphertext, and carrying out a decrypting operation to said inputted text in response to said decrypt instruction using second intermediate data at each of a plurality of decrypting stages of said decrypting operation to produce a plaintext, wherein said encrypting and decrypting operation section outputs encrypting stage data indicating an encrypting state at each of said plurality of encrypting stages and outputs decrypting stage data indicating a decrypting state at each of said plurality of decrypting stages (Figure 2, Figure 12, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65, column 9 lines 24-58);

a determining section determining whether said encrypting operation at a next encrypting stage should be changed, based on said encrypting stage data at a current encrypting :stage from said encrypting and decrypting operation section, and

determining whether said decrypting operation at a next decrypting stage should be changed, based on said decrypting stage data at a current decrypting stage from said encrypting and decrypting operation section (Figure 12, column 2 line 42 – column 3 line 51, column 5 lines 1-67, column 9 lines 24-58); and

a control section changing said encryption operation at said next encrypting stage a plurality of times when it is determined that said encrypting operation at said next encrypting stage should be changed, and changing said decrypting operation at said next decrypting stage a plurality of times when it is determined that said decrypting operation at said next decrypting stage should be changed (Figure 2, Figure 4, Figure 12, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 9 lines 24-58),

wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting operation section (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein said control section changes said intermediate data at said next encrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said current decrypting stage from said decrypting operation section (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next decrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein said control section changes said intermediate data at said next decrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 22, Aikawa discloses:

An encrypting method comprising:

(a) determining whether an encrypting operation at a current encrypting stage should be changed, based on encrypting stage data at a previous encrypting stage, said encrypting stage data at said previous encrypting stage indicating an encrypting state at said previous encrypting stage (column 2 line 42 – column 3 line 51, column 5 lines 1-67);

(b) changing said encrypting operation at said current encrypting stage when it is determined that said encrypting operation at said current encrypting stage should be

changed (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50);

(c) carrying out said encrypting operation at said current encrypting stage a plurality of times to a plaintext using intermediate data at said current encrypting stage (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65); and

(d) executing said steps (a) to (c) to each of a plurality of said encrypting stages of said encrypting operation to produce a ciphertext (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65),

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 29, Aikawa discloses:

A decrypting method comprising:

(a) determining whether a decrypting operation at a current decrypting stage should be changed, based on decrypting stage data at a previous decrypting stage, said decrypting stage data at said previous decrypting stage indicating an decrypting state at each of said plurality of processing stages (Figure 12, column 9 lines 24-58);

(b) changing said decrypting operation at said current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed (Figure 12, column 9 lines 24-58);

(c) carrying out said decrypting operation at said current decrypting stage a plurality of times to a ciphertext using intermediate data at said current decrypting stage (Figure 12, column 9 lines 24-58); and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a plaintext (Figure 12, column 9 lines 24-58),

wherein step (b) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting data at said current decrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 36, Aikawa discloses:

An encrypting and decrypting method comprising:

(a) determining whether an inputted instruction is an encrypt instruction or a decrypt instruction (Figure 2, Figure 12, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65, column 9 lines 24-58);

(b) determining whether said encrypting operation to a text at a current encrypting stage of an encrypting operation should be changed, based on said encrypting stage data at a previous encrypting stage, said encrypting stage data at said current encrypting stage indicating an encrypting state at said current encrypting stage (column 2 line 42 – column 3 line 51, column 5 lines 1-67);

(c) changing said encrypting operation to said text at said current encrypting stage when it is determined that said encrypting operation to said text at said current encrypting stage should be changed (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50);

(d) carrying out said encrypting operation to said text using first intermediate data at current encrypting stage of said encrypting operation (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

e) executing said steps (b) to (d) for each of a plurality of encrypting stages of said encrypting operation to said text in response to said encrypt instruction to produce a ciphertext (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage (Figure 12, column 9 lines 24-58);

(g) changing said decrypting operation to said text at said current decrypting stage when it is determined that said decrypting operation to said text at said current decrypting stage should be changed (Figure 12, column 9 lines 24-58);

(h) carrying out said decrypting operation to said text using second intermediate data at said current decrypting stage (Figure 12, column 9 lines 24-58); and

(i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting operation to said text in response to said decrypt instruction to produce a plaintext (Figure 12, column 9 lines 24-58)

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein step (f) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting data at said current decrypting stage from said step (h) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (f), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 43, Aikawa discloses:

A recording medium which stores a problem for an encrypting method, wherein said encrypting method comprises:

(a) determining whether an encrypting operation at a current encrypting stage should be changed, based on encrypting stage data at a previous encrypting stage, said encrypting stage data at said previous encrypting stage indicating an encrypting state at said previous encrypting stage (column 2 line 42 – column 3 line 51, column 5 lines 1-67);

(b) changing said encrypting operation at said current encrypting stage when it is determined that said encrypting operation at said current encrypting stage should be

changed (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50);

(c) carrying out said encrypting operation at said current encrypting stage a plurality of times to a plaintext using intermediate data at said current encrypting stage (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65); and

(d) executing said steps (a) to (c) to each of a plurality of said encrypting stages of said encrypting operation to produce a ciphertext (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65),

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 50, Aikawa discloses:

A recording medium which stores a program for a decrypting method, wherein said decrypting method comprises:

(a) determining whether a decrypting operation at a current decrypting stage should be changed, based on decrypting stage data at a previous decrypting stage, said decrypting stage data at said previous decrypting stage indicating an decrypting state at each of said plurality of processing stages (Figure 12, column 9 lines 24-58);

(b) changing said decrypting operation at said current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed (Figure 12, column 9 lines 24-58);

(c) carrying out said decrypting operation at said current decrypting stage to a ciphertext using intermediate data at said current decrypting stage (Figure 12, column 9 lines 24-58); and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a plaintext (Figure 12, column 9 lines 24-58),

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next decrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Regarding claim 57, Aikawa discloses:

A recording medium which stores a problem for an encrypting and decrypting method, wherein said encrypting and decrypting method comprises:

(a) determining whether an inputted instruction is an encrypt instruction or a decrypt instruction (Figure 2, Figure 12, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65, column 9 lines 24-58);

(b) determining whether said encrypting operation to a text at a current encrypting stage of an encrypting operation should be changed, based on said encrypting stage data at a previous encrypting stage, said encrypting stage data at said current encrypting stage indicating an encrypting state at said current encrypting stage (column 2 line 42 – column 3 line 51, column 5 lines 1-67);

(c) changing said encrypting operation to said text at said current encrypting stage when it is determined that said encrypting operation to said text at said current encrypting stage should be changed (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50);

(d) carrying out said encrypting operation to said text using first intermediate data at current encrypting stage of said encrypting operation (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

(e) executing said steps (b) to (d) for each of a plurality of encrypting stages of said encrypting operation to said text in response to said encrypt instruction to produce a ciphertext (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage (Figure 12, column 9 lines 24-58);

(g) changing said decrypting operation to said text at said current decrypting stage when it is determined that said decrypting operation to said text at said current decrypting stage should be changed (Figure 12, column 9 lines 24-58);

(h) carrying out said decrypting operation to said text using second intermediate data at said current decrypting stage (Figure 12, column 9 lines 24-58); and

(i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting operation to said text in response to said decrypt instruction to produce a plaintext (Figure 12, column 9 lines 24-58),

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein step (f) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting data at said current decrypting stage from said step (h) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (f), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Aikawa discloses:

An encrypting apparatus according to claim 1, wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed based on whether or not said current encrypting state from said encrypting operation section is determined to be a stage to

determine a random number conditional branch (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Aikawa discloses:

An encrypting apparatus according to claim 1, wherein said determining section determines whether an encrypting procedure at said next encrypting stage of said encrypting operation should be changed depending on at least a random number, based on said encrypting stage data at said current encrypting stage from said encrypting operation section (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35); and

wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plurality of random numberss (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 10 lines 1-35).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Aikawa discloses:

A decrypting apparatus according to claim 8, wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed based on whether or not said current

decrypting stage from said decrypting operation section is determined to be a stage to determine a random number conditional branch (Figure 12, column 9 lines 24-58).

Claim 11 is rejected as applied above in rejecting claim 8. Furthermore, Aikawa discloses:

A decrypting apparatus according to claim 8, herein said determining section determines whether a decrypting procedure at said next decrypting stage of aid decrypting operation should be changed depending n at least a random number, based on said stage data at said current decrypting stage from said decrypting operation section (Figure 12, column 9 lines 24-58); and

wherein said control section changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said plurality of random numberss (Figure 12, column 9 lines 24-58).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Aikawa discloses:

An encrypting and decrypting apparatus according to claim 15, wherein said determining section determines whether said first intermediate data at said next encrypting stage of said encrypting operation should be changed depending a first plurality of random numbers, based on whether or not said current encrypting stage from said encrypting and decrypting operation section is determined to be a stage to determine a random number conditional branch, and said determining section

determines whether said second intermediate data at said next decrypting stage of said decrypting operation should be changed depending on a second plurality of random numbers, based whether or not said current decrypting stage from said encrypting and decrypting operation section is determined to be a stage to determine a random number conditional branch (column 3 lines 34-43, column 5 line 38 – column 6 line 67, column 9 lines 24-58, column 10 lines 1-35).

Claim 18 is rejected as applied above in rejecting claim 15. Furthermore, Aikawa discloses:

An encrypting and decrypting apparatus according to claim 15, wherein said determining section determines whether an encrypting procedure at said next encrypting, stage of said encrypting operation should be changed depending on a first plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting and decrypting operation section, and determines whether a decrypting procedure at said next decrypting stage of said decrypting operation should be changed depending on a second plurality random numbers, based on said decrypting stage data at said current decrypting stage from said encrypting and decrypting operation section (Figure 4, Figure 12, column 3 lines 44-46, column 5 lines 17-50, column 9 24-58, column 10 lines 1-35); and

wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said first plurality of random numbers and changes said decrypting procedure at said next decrypting stage

of said decrypting operation depending on said second plurality of random numbers (Figure 2, Figure 4, Figure 12, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 9 lines 24-58, column 10 lines 1-35).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Aikawa discloses:

An encrypting method according to claim 22, wherein said determining section includes:

determining whether said intermediate data at said current encrypting stage of said encrypting operation should be changed depending on at a plurality of random numbers, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35).

Claim 25 is rejected as applied above in rejecting claim 22. Furthermore, Aikawa discloses:

An encrypting method according to claim 22, wherein said determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35); and

wherein said changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said plurality of random numbers (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 10 lines 1-35).

Claim 30 is rejected as applied above in rejecting claim 29. Furthermore, Aikawa discloses:

A decrypting method according to claim 29, wherein said determining includes:

determining whether said intermediate data at said current decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58).

Claim 32 is rejected as applied above in rejecting claim 29, wherein said determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58); and,

wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Aikawa discloses:

An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether said first intermediate data at said current encrypting stage of said encrypting operation should be changed depending on at least a first random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35);

wherein said (f) determining includes:

determining whether said second intermediate data at said current decrypting stage of said decrypting operation should be changed depending on at least a second random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58);

wherein said encrypting stage data includes said first intermediate data at said current encrypting stage and said decrypting stage data includes said second intermediate data for said current decrypting stage (column 3 lines 34-43);

wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said first random number (Figure 3, Figure 12, column 5 line 38 – column 6 line 6); and

wherein said (g) changing includes:

hanging said second intermediate data at said current decrypting stage depending on said second random number (Figure 12, column 9 lines 24-58).

Claim 39 is rejected as applied above in rejecting claim 36. Furthermore, Aikawa discloses:

An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on at least a first random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35);

wherein said (f) determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on at least a second random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58);

wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said first random number (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 10 lines 1-35); and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said second random number (Figure 12, column 9 lines 24-58).

Claim 44 is rejected as applied above in rejecting claim 43. Furthermore, Aikawa discloses:

A recording medium according to claim 43, wherein said determining includes:

determining whether said intermediate data at said current encrypting stage of said encrypting operation should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35);

wherein said encrypting stage data includes said intermediate data at said current encrypting stage (column 3 lines 34-43), and

wherein said changing includes:

changing said intermediate data at said current encrypting stage depending on said plurality of random numbers (Figure 3, column 5 line 38 – column 6 line 67).

Claim 46 is rejected as applied above in rejecting claim 43. Furthermore, Aikawa discloses:

A recording medium according to claim 43, wherein said determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35); and

wherein said changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said plurality of random numbers (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 10 lines 1-35).

Claim 51 is rejected as applied above in rejecting claim 50. Furthermore, Aikawa discloses:

A recording medium according to claim 50, wherein said determining section includes:

determining whether said intermediate data at said current decrypting stage of said decrypting operation should be changed depending on a plurality of random numbers, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58).

Claim 53 is rejected as applied above in rejecting claim 50. Furthermore, Aikawa discloses:

A recording medium according to claim 50, wherein said determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58); and

wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 58 is rejected as applied above in rejecting claim 57. Furthermore, Aikawa discloses:

A recording medium according to claim 57, wherein said (b) determining includes:

determining whether said first intermediate data at said current encrypting stage of said encrypting operation should be changed depending on at least a first random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35);

wherein said (f) determining includes:

determining whether said second intermediate data at said current decrypting stage of said decrypting operation should be changed depending on at least a second random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58);

wherein said encrypting stage data includes said first intermediate data at said current encrypting stage and said decrypting stage data includes said second intermediate data for said current decrypting stage;

wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said first random number (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 10 lines 1-35); and

wherein said (g) changing includes:

changing said second intermediate data at said current decrypting stage depending on said second random number (Figure 12, column 9 lines 24-58).

Claim 60 is rejected as applied above in rejecting claim 57. Furthermore, Aikawa discloses:

A recording medium according to claim 57, wherein said (b) determining includes:

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on at least a first random number, based on said encrypting stage data at said previous encrypting stage (Figure 4, column 3 lines 44-46, column 5 lines 17-50, column 10 lines 1-35);

wherein said (f) determining includes:

determining whether a decrypting procedure at said current decrypting stage of said decrypting operation should be changed depending on at least a second random

number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58);

wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said first random number (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50, column 10 lines 1-35); and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said second random number (Figure 12, column 9 lines 24-58).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Aikawa discloses:

An encrypting apparatus according to claim 2, wherein said control section changes said intermediate data at said next encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers (column 3 lines 34-43, column 5 line 38 – column 6 line 67, column 10 lines 1-35).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Aikawa discloses:

An encrypting apparatus according to claim 4, wherein said control section changes said encrypting procedure at said next encrypting stage encrypting operation depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers (Figure 2, Figure 4, column 2 lines 27-65, column 5 lines 1-50, column 10 lines 1-32).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Aikawa discloses:

A decrypting apparatus according to claim 9, wherein said control section changes said intermediate data at said next decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Aikawa discloses:

A decrypting apparatus according to claim 11, wherein said control section changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Aikawa discloses:

An encrypting and decrypting apparatus according to claim 16, wherein said control section changes said first intermediate data at said next encrypting stage depending on said inputted text or a data dependent on said inputted text in place of said first random number, and changes said second intermediate data at said next decrypting stage depending on said inputted text or said data dependent on said inputted text in place of said second random number (Figure 2, Figure 4, Figure 12, column 2 lines 27-65, column 5 lines 1-50, column 9 lines 24-58, column 10 lines 1-32).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Aikawa discloses:

An encrypting and decrypting apparatus according to claim 18, wherein said control section changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said inputted text or a data dependent on said inputted text in place of said first random number, and changes said decrypting procedure at said next decrypting stage of said decrypting operation depending on said inputted text or said data dependent on said inputted text in place of said second random number (Figure 2, Figure 4, Figure 12, column 2 lines 27-65, column 5 lines 1-50, column 9 lines 24-58, column 10 lines 1-32).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Aikawa discloses:

An encrypting method according to claim 23, wherein said changing includes:

changing said intermediate data at said current encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers (column 3 lines 34-43, column 5 line 38 – column 6 line 67, column 10 lines 1 – 35).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Aikawa discloses;

An encrypting method according to claim 25, wherein said changing includes:

changing said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers (Figure 2, Figure 4, column 2 lines 27-65, column 5 lines 1-50, column 10 lines 1-32).

Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Aikawa discloses:

A decrypting method according to claim 30, wherein said changing includes:

changing said intermediate data at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Aikawa discloses:

A decrypting method according to claim 32, wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 38 is rejected as applied above in rejecting claim 37. Furthermore, Aikawa discloses:

An encrypting and decrypting method according to claim 37, wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said text or a data dependent on said text in place of said first random number (column 3 lines 34-43, column 5 line 38 – column 6 line 67, column 10 lines 1-35); and

changing said second intermediate data at said current decrypting stage depending on said text or said data dependent on said text in place of said second random number (Figure 12, column 9 lines 24-58).

Claim 40 is rejected as applied above in rejecting claim 39. Furthermore, Aikawa discloses:

An encrypting and decrypting method according to claim 39, wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said text or a data dependent on said text in place of said first random number (Figure 2, Figure 4, column 2 lines 27-65, column 5 lines 1-50, column 10 lines 1-35); and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said text or said data dependent on said text in place of said second random number (Figure 12, column 9 lines 24-58).

Claim 45 is rejected as applied above in rejecting claim 44. Furthermore, Aikawa discloses:

A recording medium according to claim 44, wherein said changing includes:

changing said intermediate data at said current encrypting stage depending on said plaintext or a data dependent on said plaintext in place of said plurality of random numbers (column 3 lines 34-43, column 5 line 38 – column 6 lines 67, column 10 lines 1-35).

Claim 47 is rejected as applied above in rejecting claim 46. Furthermore, Aikawa discloses:

A recording medium according to claim 46, wherein said changing includes:

changes said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plaintext or a data dependent on said plaintext

in place of said plurality of random numbers (Figure 2, Figure 4, column 2 lines 27-65, column 5 lines 1-50, column 10 lines 1-35).

Claim 52 is rejected as applied above in rejecting claim 51. Furthermore, Aikawa discloses:

A recording medium according to claim 51, wherein said changing includes: changing said intermediate data at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 54 is rejected as applied above in rejecting claim 53. Furthermore, Aikawa discloses:

A recording medium according to claim 53, wherein said changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said ciphertext or a data dependent on said ciphertext in place of said plurality of random numbers (Figure 12, column 9 lines 24-58).

Claim 59 is rejected as applied above in rejecting claim 58. Furthermore, Aikawa discloses:

A recording medium according to claim 58, wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said text or a data dependent on said text in place of said first random number (Figure 2, Figure 4, column 2 lines 27-65, column 5 lines 1-50, column 10 lines 1-35); and

wherein said (g) changing includes:

changing said second intermediate data at said current decrypting stage depending on said text or said data dependent on said text in place of said second random number (Figure 12, column 9 lines 24-58).

Claim 61 is rejected as applied above in rejecting claim 60. Furthermore, Aikawa discloses:

A recording medium according to claim 60, wherein said (c) changing includes:

changing said encrypting procedure at said current encrypting stage of said encrypting operation depending on said text or a data dependent on said text in place of said first random number (Figure 2, Figure 4, column 2 lines 27-65, column 5 lines 1-50, column 10 lines 1-35); and

wherein said (g) changing includes:

changing said decrypting procedure at said current decrypting stage of said decrypting operation depending on said text or said data dependent on said text in place of said second random number (Figure 12, column 9 lines 24-58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 6-7, 13-14, 20-21, 27-28, 34-35, 41-42, 48-49, 55-56, and 62-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aikawa et al. (U.S. Patent 6,606,385) in view of Ishii et al. (U.S. Patent 6,175,850).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Aikawa discloses:

An encrypting apparatus according to claim 1, wherein said determining section determines whether said encrypting operation at said next encrypting stage should be changed depending on at least a random number, based on said encrypting stage data

at said current encrypting stage from said encrypting operation section (Figure 4 column 5 lines 17-50, column 3 lines 44-46, column 10 lines 1-32).

Aikawa does not explicitly teach inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers. Ishii discloses inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting operation.

Claim 7 is rejected as applied above in rejecting claim 6. Aikawa does not explicitly teach an encrypting apparatus wherein said control section inserts a delay time in an encrypting operation at a next encrypting stage depending on a plaintext or a data dependent in place of a random number. Ishii discloses inserting a delay time in said

encrypting operation at said next encrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting operation.

Claim 13 is rejected as applied above in rejecting claim 8. Furthermore, Aikawa discloses:

A decrypting apparatus according to claim 8, wherein said determining section determines whether said decrypting operation at said next decrypting stage should be changed depending on at least a random number, based on said stage data at said current decrypting stage from said decrypting operation section (Figure 12, column 9 lines 24-58).

Aikawa does not explicitly teach inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers. Ishii discloses inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in a decrypting operation.

Claim 14 is rejected as applied above in rejecting claim 13. Aikawa does not explicitly teach a decrypting apparatus wherein said control section inserts a delay time in an decrypting operation at a next decrypting stage depending on a plaintext or a data dependent in place of a random number. Ishii discloses inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii

teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in a decrypting operation.

Claim 20 is rejected as applied above in rejecting claim 15. Furthermore, Aikawa teaches:

An encrypting and decrypting apparatus according to claim 15, wherein said determining section determines whether said encrypting operation at said next encrypting stage should be changed depending on at least a first random number, based on said encrypting stage data at said current encrypting stage from said encrypting and decrypting operation section, and determines whether said decrypting operation at said next decrypting stage should be changed depending on at least a second random number, based on said decrypting stage data at said current decrypting

stage from said encrypting and decrypting operation section (Figure 4, Figure 12, column 5 lines 17-50, column 3 lines 44-46, column 9 lines 24-58, column 10 lines 1-32).

Aikawa does not explicitly teach inserting a first delay time in said encrypting operation at said next encrypting stage depending on said first random number and inserts a second delay time in said decrypting operation at said next decrypting stage depending on said second random number. Ishii discloses inserting a delay time in encrypting/decrypting operations at encrypting/decrypting stages(Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting/decrypting operation.

Claim 21 is rejected as applied above in rejecting claim 20. Aikawa does not explicitly teach an encrypting/decrypting apparatus wherein said control section inserts a delay time in an encrypting/decrypting operation at a next encrypting/decrypting stage depending on a plaintext or a data dependent in place of a random number. Ishii discloses inserting a delay time in said encrypting/decrypting operation at said next encrypting/decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting/decrypting operation.

Claim 27 is rejected as applied above in rejecting claim 22. Furthermore, Aikawa discloses:

An encrypting method according to claim 22, wherein said determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage (Figure 4 column 5 lines 17-50, column 3 lines 44-46, column 10 lines 1-32).

Aikawa does not explicitly teach inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers. Ishii discloses inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting operation.

Claim 28 is rejected as applied above in rejecting claim 27. Aikawa does not explicitly teach an encrypting method wherein said control section inserts a delay time in an encrypting operation at a next encrypting stage depending on a plaintext or a data dependent in place of a random number. Ishii discloses inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting operation.

Claim 34 is rejected as applied above in rejecting claim 29. Furthermore, Aikawa discloses:

A decrypting method according to claim 29, wherein said determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58). Aikawa does not explicitly teach inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers. Ishii discloses inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in a decrypting operation.

Claim 35 is rejected as applied above in rejecting claim 34. Aikawa does not explicitly teach a decrypting method wherein said control section inserts a delay time in an decrypting operation at a next decrypting stage depending on a plaintext or a data

dependent in place of a random number. Ishii discloses inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in a decrypting operation.

Claim 41 is rejected as applied above in rejecting claim 36. Furthermore, Aikawa discloses:

An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on at least a first random number, based on said encrypting

stage data at said previous encrypting stage (Figure 4 column 5 lines 17-50, column 3 lines 44-46, column 10 lines 1-32);

wherein said (f) determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on at least a second random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58);

Aikawa does not explicitly disclose inserting a first delay time in said encrypting operation at said current encrypting stage depending on said first random number, and wherein said (g) changing includes: inserting a second delay time in said decrypting operation at said current decrypting stage depending on said second random number. Ishii discloses inserting a delay time in encrypting/decrypting operations at encrypting/decrypting stages (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would

have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting/decrypting operation.

Claim 42 is rejected as applied above in rejecting claim 41. Aikawa does not explicitly discloses an encrypting and decrypting method according to claim 41, wherein (c) changing includes inserting a first delay time in an encrypting operation at a current encrypting stage depending on text or a data dependent on the text and wherein (f) changing includes inserting a second delay time in said decrypting operation at said current decrypting stage depending on text or data dependent on the text. Ishii discloses inserting a delay time in said encrypting/decrypting operation at said next encrypting/decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay

inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting/decrypting operation.

Claim 48 is rejected as applied above in rejecting claim 43. Furthermore, Aikawa discloses:

A recording medium according to claim 43, wherein said determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage (Figure 4 column 5 lines 17-50, column 3 lines 44-46, column 10 lines 1-32).

Aikawa does not explicitly teach inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers. Ishii discloses inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by

Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting operation.

Claim 49 is rejected as applied above in rejecting claim 48. Aikawa does not explicitly teach a recording medium wherein changing inserts a delay time in an encrypting operation at a next encrypting stage depending on a plaintext or a data dependent in place of a random number. Ishii discloses inserting a delay time in said encrypting operation at said next encrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting operation.

Claim 55 is rejected as applied above in rejecting claim 50. Furthermore, Aikawa discloses:

A recording medium according to claim 50, wherein said determining includes: determining whether said decrypting operation at said current decrypting stage should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58).
Aikawa does not explicitly teach inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers. Ishii discloses inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35,

column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in a decrypting operation.

Claim 56 is rejected as applied above in rejecting claim 55.

Aikawa does not explicitly teach a recording medium where changing includes inserting a delay time in an decrypting operation at a next decrypting stage depending on a plaintext or a data dependent in place of a random number. Ishii discloses inserting a delay time in said decrypting operation at said next decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in a decrypting operation.

Claim 62 is rejected as applied above in rejecting claim 57. Furthermore, Aikawa discloses:

A recording medium wherein said (b) determining includes:

determining whether said encrypting operation at said current encrypting stage should be changed depending on at least a first random number, based on said encrypting stage data at said previous encrypting stage (Figure 4 column 5 lines 17-50, column 3 lines 44-46, column 10 lines 1-32);

wherein said (f) determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on at least a second random number, based on said decrypting stage data at said previous decrypting stage (Figure 12, column 9 lines 24-58).

Aikawa does not explicitly disclose inserting a first delay time in said encrypting operation at said current encrypting stage depending on said first random number, and wherein said (g) changing includes: inserting a second delay time in said decrypting operation at said current decrypting stage depending on said second random number. Ishii discloses inserting a delay time in encrypting/decrypting operations at encrypting/decrypting stages (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203)

determines a delay time to be added to the encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting/decrypting operation.

Claim 63 is rejected as applied above in rejecting claim 62. Aikawa does not explicitly discloses an encrypting and decrypting method according to claim 62, wherein (c) changing includes inserting a first delay time in an encrypting operation at a current encrypting stage depending on text or a data dependent on the text and wherein (f) changing includes inserting a second delay time in said decrypting operation at said current decrypting stage depending on text or data dependent on the text. Ishii discloses inserting a delay time in said encrypting/decrypting operation at said next encrypting/decrypting stage depending on said plurality of random numbers (Figure 7, Figure 8, column 10 line 37 – column 13 line 15). Ishii teaches a delay insertion method that incorporates a random number generator to provide an additional measure of randomness in conjunction with an initial value supplied to the device either externally or internally. These initial values could be determined from a plaintext or a data dependent. With these inputs of the random number and the initial value, the delay time determining unit (Figure 7 item 203) determines a delay time to be added to the

encryption/decryption processing. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the delay inserting apparatus of Ishii with the invention of Aikawa. The motivation for combination given by Ishii is to prevent the timing attacks on cryptography systems (column 2 lines 11-35, column 13 lines 8-15). Therefore, it would have been obvious to combine the delay inserting apparatus of Ishii with Aikawa to insert a delay time in an encrypting/decrypting operation.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
12/06/04

EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136